

Comment to the FCC on proceeding 16-251 the search for obsolete rules.

See FCC document FCC-01-160A1.pdf. This document delineates the rule I believe is obsolete and should be removed. It says 'this receiver may not be modified to receive cellular communications'. They mean Analog cellular communications. However, there are no more Analog cellular signals that these type of receivers could be used to receive. That has been shut down for years. So, why do we have this rule persisting? Even if it was updated for digital cellular the digital cellular signals have never been applied to this ruling. The rule does not even state precise frequency bands, and those have changed. It should not be applied to this type of receiver FDMA channelized scanning, since the bandwidth and signal processing is missing in these receivers that would be needed to decode cell signals. Beyond that the vocoders and despanders do not exist in this type of hardware.

Bands that were excluded: 825-845 870-890 Some models: 825-849, 870-894

Other models 825-849, 867-894

* in Nextel rebanded areas, digital cellular moved into these bands, Midwest: 862-869 yet some existing radios had this band in them,

In a recent *2005* digital trunking scanner, it still has 868.9875 so now there is overlap of this band, 862-868.9875, no action or correction from the FCC it is not paying attention. Oh but its digital cellular, so who cares? Well I do, thanks for not asking me.

The avenue by which the scanning receiver is regulated is that it may radiate RF energy.

Newer designs radiate so little energy they are difficult to detect or find where they are radiating.

Most of the newly designed scanners have Triple conversion receivers have filters such that the local oscillator RF leakage radiation is hard to detect with another receiver even a few feet away. That assumes the frequencies to look for it are known. The older single conversion scanning receivers were 70db worse than the new triple conversion receivers. There was very little isolation between the antenna and the local oscillator in the single conversion radios. If you can't measure any RF radiation above a threshold level than maybe part 15 does not even apply to these receivers because of such low emissions. They are designed to be low emission to reduce spurious points that jam narrow band channels. So they tend to be very well shielded internally.

This document FCC-01-160A1 states scanning receivers must not be modified to receive cellular communications.

Due to the conversion to CDMA LTE and other digital formats, I say this is impossible. Even if the radio tunes these frequencies the decoding of voice from it is not possible, and it never has been.

This rule was written during a period when there were mostly analog cellular signals in the 825-845 and 870-890 bands. The rule applied only to new scanning receivers built after that date May 22, 2001, or scanners, not to Two way radio that did not have bands in that range.

This time is long gone and there are no analog cellular signals. So, you no longer need to exclude any frequency from these radios. The manufacturers have been excluding unused bands to cut costs, so these type of radios would not matter as much as a general coverage receiver/scanner. So a receiver

often can scan but typically covers all frequencies, because the user needs them for some purpose other than receiving digital cellular. Perhaps to look at the analog aspects of the digital signals, determine what is in use, or use with a frequency converter such as could be used with satellite downlinks.

Reception of a wide band cellular signal is impossible with these receivers. Detection of parts of the signal is possible, but not useful to decode voice. It is possible to do discriminator taps to feed narrowband formats such as P25, Turbo, NXDN into an external decoder, but again the filter bandwidths are too narrow and a wide band format such as digital cellular would not be passed through at the proper bandwidth and frequency spectrum to be decoded.

There are some corporations making products that emulate cell towers such as Harris, they can probably do cell tower encoding and maybe decoding, but this is not possible within the realm of a typical scanning radio user.

An advanced radio user or enthusiast or amateur has uses for these receivers and this group of people were the most affected by these rules.

This rule did nothing to secure the analog signals. If you already had a receiver you could still pick them up. What the rules did do was severely handicap the receive bands of some models of radio or scanning equipment, make them harder to repair, damage the market for the radios, and the rule has never been updated since that document. It stinks like an old shoe.

Since that time a lot has changed, which demonstrates this rule is no longer of concern to the cell companies or the government, perhaps because the cell signals can't be decoded with scanning radios.

How did this affect some radios?

Icom R3, a combo video/analog receiver covering 30-2450 except 815-902.

Because of its spurious reception nearly the entire 800 band where most push to talk radio has migrated, was excluded. I have one of these but was only interested in it due to the analog TV capability. Note though the digital cellular referred to as PCS in 1775-1975 mhz was left in the receive band. The radio is analog, so other than detecting there is a signal it does not decode any of the digital cellular format. The signals in the PCS band appear the same as those in the 800 band digital cellular.

It does detect these signals and is helpful to determine where your cellular signal is coming from, and also useful to determine if a given cell tower has your band on it or not.

Intermediate Frequency taps could be made in these radios but only bandwidths of 200khz or less were usable for decoding digital signals of the narrowband type. They do not have wide filters. Some spectrum analyzers have these wide filters but unless they have specific hardware they do not decode or test digital cellular signals. I note a lot of TDMA was retired and along with that cellular format being shut down, so a lot of the test equipment was retired.

Radios that were negatively impacted by the rule:

Examples: Icom R20, an all mode analog receiver, 0.5mhz – 3002 mhz, with 825-845 and 866-896. This receiver was missing the top MHz (866-867) of conventional 800mhz allocation. It did not have spurious

but before Nextel rebanding these channels were used in 2way radio.

I think it was an error by the programmers in Japan. In some areas of the US 862-867 was 'reband' and allocated to NEXTEL due to its severe interference when interleaved in the 851-867 band.

That 862-870 band and Nextel was purchased by Sprint so Nextel was shut down and replaced with CDMA Cellular, each of the CDMA carriers is approximately 1 mhz wide so 2 or 3 of those were placed in this band in some areas of the US at least Iowa and not in busy metro areas that did not have Nextel. Now it has wound up with the same waveform as the band above but was 'moved into range' of the analog and digital receivers that are sold today. No problem they don't decode it, just sounds like white noise. And it's exactly the same waveform as above I checked it out on spectrum analyzers. A 1mhz wide signal with a little ripple across the band, in SSB has a slight buzzing sound to it. Each type has its own sound, so a 3G is a bit different than a CDMA, and a 4G or LTE is wider than that, I can type that in this Icom R20 as it predates the band and no new regulation was made to exclude it, why would you need to, the radios must be specifically designed to receive this type of signal, but the scanning receiver is not. They can detect small parts of the signal is there, and that's it. They may be able to tell by the sound that there is activity, but that's not harmful to anyone...

So some scanning receivers still in use today 'receive' the frequency bands but due to the narrow IF bands less than 200khz, they simply detect the digital cellular signal without decoding it.

So the 'cellular telephone' has moved into the bands still allowed by this rule in some areas with no consequence. And the 'PCS' bands essentially cellular bands (they do the same thing) have not been 'tapped' by these receivers.

Also, the 1.8-2.0 ghz spectrum has always been in some models of the scanning receivers if they had a high enough bandwidth, but since cellular signals have their bandwidth spread by CDMA and digital encoded, it is not received but can be detected.

So, if there is no concern over these narrow band radios tuning the PCS spectrum then why is there concern over them tuning the 825-845 and 862-894 bands? These carry the exact same cdma signal format as do the 1.775-2.0ghz spectrum. Many phones now do both bands.

And if there is no concern over them tuning the 3G and 4G and LTE bands (700-800) which many do, then the same is true for the 825-845 and 862-894 bands.

The encoding methods used in CDMA are incompatible with the bandwidth and decoding capability of narrow band scanners. The latest scanners tend to cover only bands of interest, but general coverage receivers cover every band except cellular. These receivers are useful for many purposes that require the complete band coverage including the digital cellular bands.

There are no more usage of analog cellular in USA or Canada. Since the rules did not have the ability to remove older receivers that could receive all frequency bands, these still exist today in a large percentage of the original builds of these. So the Rules did not really protect these signals, more along the lines warn scanner receivers not to reveal any phone calls they heard, (but wasn't there already a

law for that., but it is likely when the cellular carriers converted away from analog that there is no evidence anyone is decoding cell signals. True security was not implemented with cryptography until recent voip apps could be loaded onto a cellphone that provide end to end encryption and used its data connection to connect two users. There is something called voice privacy which means some kind of added encryption is added to a vocoder that may help scramble the connection between a cell tower and the cellphone, but would have no effect on the land line part of it, so without end to end encryption (these days AES 2048 bits may be adequate)

These scanning receivers that tune to the cellular uplinks can be used to determine when your cellphone is transmitting. That is useful for signal security and may tell you your phone is compromised, or if its transmitting when you don't expect it, or you have something enabled that is undesirable, so these receivers may benefit the user (is that who we care about?) in that they know something is wrong when the phone is doing more than pinging a tower when its not in use (phone compromised and listening to you) Or to let you know you have some app that is probably transmitting voice to a server (apple iPhone – all SIRI queries go to the apple cloud! Android voice commands are dealt with on the phone locally. However the query or command may be transmitted.

What are the receivers used for and why do you need all frequency bands?

The R3 can tune analog cable and receive any clear channels, and these systems extend to 1 Ghz.

Scanning for information related to incidents, road blockages, bad driving conditions, traffic congestion, and incidents near ones home, police chases, and more. If part or all of a band is 'cut out' you cant use it.

These calls are very useful when choosing a route to drive, or to determine that there is a road condition that is not reported anywhere else. Some small counties and low population states have police dispatch, that is basically the only source of this type of information, because there isn't anyone else there to report it, and police are responding to an incident and do not have duties that include informing the public, but the public can benefit from the dispatch. The great digital conversion has brought with it encryption of some or all channels so this deprives the public of information it has use for, and in fact has paid for.

General coverage receivers can be used for many things.

These can be used for testing transmitters, checking for spurious, testing antennas, determining signal strengths and the direction its coming from. For a cell user one might be able to optimize reception by finding the uplink channel, tuning to the corresponding downlink and determining the direction its coming from. This is hard to do with a cellphone (debug mode is different on all of them) and has time delay, but an analog receiver can peak up on the noise spectrum using a directional antenna. It can test the antenna (noise increase in receiver shows the existence of a signal) Locate interference(not a large factor in CDMA phones) and locate cell jammers which were imported into the country.

Analog is still in use on many radio bands.

These receivers can be used with frequency converters some of which cover a much wider band including all of 800mhz. Here excluded bands are a problem.

I believe this scanner rulemaking started when Newt Gingrich was overheard and recorded doing something he should not have by his political opponents who lived in his area and heard him on analog cellular, and it was played on the radio and TV. He probably quit using cellphones for that kind of thing until they converted to digital. The cat is already out of the bag. The radios are already out there. Their hope is eventually the radios all wear out, or the signal changes so it can't be heard. The result is what I call 'Vandalization' of scanners.

Since that time in the 2000 time frame, there is no longer any analog cellular in use anywhere I've checked including several foreign countries and many states in the USA. I have been through a large part of the country from east to west and have not heard analog cell for at least 10-15 years. Clearly there is no way to add a cdma decoder to a scanning receiver. Numerous problems would crop up, Chipsets are required, access to data on them is very restricted, wider bandwidths are required, Despreading or de-hopping data demod is required. For the most part the bandwidths and frequency scheme and filter set is incorrect in the latest set of receivers I've looked at. There are two types of scanners most commonly purchased, Analog general coverage, and digital trunking scanners. For signal work the analog is preferred, and for modern signal waveforms the digital trunking is a must. Most of the digital trunk type just cover the common two way bands.

This rulemaking is obsolete, clearly there is no problem with analog or even narrowband digital scanners and cellular phone interception. If you really are concerned with this, you can buy phones with end to end encryption, of course that means whoever you are talking to must have it as well. From recent news reports it is clear that you better have encryption end to end if you care about security.

IF you don't need that , go ahead and use your cellphone. The mass users of these scanning radios are not likely to hear it with these narrow band radios. Since these don't decode CDMA or any other cell format there is no need for this rule.

The band is useful as stated above to some radio users, for non radiating radio uses as well as testing and tuning cellular systems and signals. Obviously digital cellular is not an analog or narrow band signal and every few years the signal format changes and everyone gets a new phone to keep up with it. These receivers are not designed and completely unable to decode CDMA which is the most popular format in the country now.

It does hurt the scanning and receiver radio industry in that they sell fewer scanners then they would, since a used radio has better capability than these new ones that are missing bands.

This should be retired and removed from the FCC rules. This is why your rules should expire unless they are re-examined and re-justified. It does not perform its stated purpose to improve cell phone security,

and creates annoyance hardship discrimination and stigmatism against users of these radios. This security can be left to the end users to decide. Most of them know about encryption now. I still know a few that refuse to bank on the internet, because they don't have a clue about encryption.

A large number of police departments, and federal narrowband radio users can encrypt if they buy that option for their new digital radios. None of the new digital scanners do more than indicate encryption but do not decode it. So if a signal needs security no questions asked they can encrypt it. Should not be a problem except there are some departments encrypting everything even that which might be useful to warn the public by allowing them to hear dispatches.

It does not change the security of a cellphone to remove this ruling because digital cellular formats are incompatible with narrowband radios. We need the FCC to clear this exclusion from radios that may be used for decades to come. This rule has no useful purpose, and it's obviously not been looked at in many years. It failed to account for PCS, changes in cellular to exclusively digital, and maintaining this rule places a stigma on the scanner owner which is without merit. Though few users could care less, those of us that do will be able to buy new radios without concern for this 800 band frequency exclusion. Since the 1.8 band signals are exactly the same format as 800 digital is now, and you have always ignored the fact these receivers do get that PCS band, then why do you need the exclusion. I have not heard of a scanning radio being used to decode digital cellular. Some models have always had 1.8-2ghz band, and nobody has reported or complained about these radios decoding cellular, because they don't. Incompatible signals can not be decoded. CDMA is incompatible. GSM is incompatible. The exact format that started out on 1.8-2ghz (CDMA) is the same format used in the 800 cell bands. There is no need for the warning, label or frequency exclusion. It has accomplished one thing, I think it is one of the stupidest rules you ever came out with because it has never protected an analog cell signal. Digital cell signals are protected by the encoding methods. This rule became obsolete when the last analog cellular signal left the air. This rule was theatre of the absurd when you add it all up. If anyone had an older radio it would pick up analog cellular. If anyone had test equipment it was unaffected. It did nothing to get rid of those. And many of these radios are still out there, I've seen them.

Given what we've heard on the news, governments and corporations spying and sniffing traffic, if you don't use end to end encryption you can't say it's private communications. Encryption is readily available for anyone who wants it – most new voice over IP apps will work on cellphones now. The cell companies answer to what their customers want, and I observe most of them aren't concerned about governments corporations or telecom workers hearing them. You would have to be a telecom engineer with access to development boards and systems to get anywhere close to casually listening to a cell signal these days, so there's probably next to nobody able to do so. I'd guess for the most part nobody wants to either given the nature of this type of traffic. And the typical phone users willingly use open WIFI with many of the phones today, which is not secure.

After testimony of Bob Grove, a seller of the receivers, FCC said manufacturers must exclude any spurious response as well as primary bands. That is what did the most 'damage' to the few radios sold

during that time. Huge chunks of useful bands were removed. Vandalized to make an example of one or two people who broke their rules.....because they heard and reported on something to gain political advantage.

I remember Newt Gingrich had a lot to do with this ruling so I don't give him much credit for helping the public. He has been on Media a lot lately and I always remember this story every time he is on the TV.

We never forget. I get reminded of this whole stupid thing every time I see the back of my radios.

Through numerous technology shifts frequencies formats signals change but old FCC rules never die, even if they barely worked in the first place. Time to get rid of this forever and do not do it again.

Oh here is a good one for you. IF you want cellular security then it has to have 4096 bit AES encryption, end to end, and lets make that true of all land lines as well, end to end public key encryption.

Just fine with me. The computing power to do that is already here now.

I think that size key is beyond anyone's ability to break it.

The reality of this rule was that if you used an analog cellphone, then assume someone could hear it.

Before that, AT&T ran VHF mobile phone systems, and you had to assume someone could hear that.

Before that there were some phone patches over analog radio, you had to assume someone could hear that.

Over and above all of this, it was the duty of anyone that overheard this not to divulge it.

Sounds like they were trying to punish a couple of people and wound up affecting others that had nothing to do with it.

Summary and conclusion

FCC is not auditing numerous rules it has created.

FCC is not expiring any rules old rules, and its buried in them, hard to find anything.

FCC is charging too much for licenses that is preventing some users from using 2 way radio

FCC is not hiring competent engineers that are familiar with state of the art.

FCC does not venture far from DC and appears unfamiliar with what is going on unless someone tells them.

FCC does not audit licenses to be sure they are used.

FCC license fees are free of charge for numerous government users, yet the FCC charges large fees to the few commercial users so they are carrying the load of FCC fees

Due to this FCC policy of free licenses for Gov. an unfair burden is placed on small business user.

FCC policy allows Numerous state, county and city governments migrate from their old licenses without terminating them and freeing the spectrum since there is no auditing and charging

FCC is forcing narrowband conversion but the digital technologies have serious issues such as high voice delay, variation between vendors, incompatibility, no improvement in interoperability, signal formats that are modified by each vendor for simulcast, that is not in the standards.

The current set of rules (fixed channel, crystal controlled) are obsolete, because most new radios are synthesized, have hundreds of channels, and most channels that are reserved are never shared.

There are not enough MURS and GMRS type channels available, to get channel use up you have to have channel flexibility.

Spectrum use is poor because everyone is on a reserved channel when they could be on a shared channel with some exceptions for larger corporations which tend to be heavy users and small business tend to be little used channels.

So more common itinerant and unlicensed channels are needed. The FRS service is so popular it should be expanded. I observe numerous businesses using FRS for their in store communications rather than 'licensed radio'. Buy them and use them, simple!

Trump has stated for every rule you create, expire 2 of them, that would be rules like this one. That would help eliminate obsolete rulemakings like this one.

C.K.

Below: One of the most vandalized radios out there, Icom R3. All but some of the uplink band in the 800mhz two way band is removed. 816-902 missing. Looks like the FCC rules spilled over into Canada as well. Really bad.

